Modulo

From Wikipedia, the free encyclopedia.

The word ***modulo*** is the Latin ablative of modulus. It was introduced into mathematics in the book *Disquisitiones Arithmeticae* by Carl Friedrich Gauss in 1801. Ever since however, "modulo" has gained many meanings, some exact and some imprecise.

- (This usage is from Gauss's book.) Given the integers a, b and n, the expression $a \equiv b \pmod{n}$ (pronounced "a is congruent to b **modulo** n") means that a and b have the same remainder when divided by n, or equivalently, that $a-b$ is a multiple of n. For more details, see modular arithmetic.
- In computing, given two integers, a and n, a **modulo** n is the remainder after numerical division of a by n, under certain constraints. See modulo operation.
- Two members of a ring or an algebra are congruent **modulo** an ideal if the difference between them is in the ideal.
- Two members a and b of a group are congruent **modulo** a normal subgroup iff ab^{-1} is a member of the normal subgroup. See quotient group and isomorphism theorem.
- Two subsets of an infinite set are **equal modulo finite sets** precisely if their symmetric difference is finite, that is, you can take a finite piece from the first infinite set, then add a finite piece to it, and get as result the second infinite set.
- The most general precise definition is simply in terms of an equivalence relation R. We say that a is *equivalent* or *congruent* to b **modulo** R if aRb.
- In the mathematical community, the word **modulo** is also used informally, in many imprecise ways. Generally, to say "A is the same as B modulo C" means, more-or-less, "A and B are the same except for differences accounted for or explained by C". See modulo (jargon).

Retrieved from "http://en.wikipedia.org/wiki/Modulo"

Categories: Mathematical terminology | Disambiguation

- This page was last modified 18:02, 28 November 2005.
-